Near-Optimal Modulo-and-Forward Scheme for the Untrusted Relay Channel

Shengli Zhang, Lisheng Fan, Mugen Peng, and H. Vincent Poor

Abstract

This paper studies an untrusted relay channel, in which the destination sends artificial noise simultaneously with the source sending a message to the relay, in order to protect the source's confidential message. The traditional amplify-and-forward (AF) scheme shows poor performance in this situation because of the interference power dilemma: providing better security by using stronger artificial noise will decrease the confidential message power from the relay to the destination. To solve this problem, a modulo-and-forward (MF) operation at the relay with nested lattice encoding at the source is proposed. For this system with full channel state information at the transmitter (CSIT), theoretical analysis shows that the proposed MF scheme approaches the secrecy capacity within $1/2$ bit for any channel realization, and hence achieves full generalized security degrees of freedom (G-SDoF). In contrast, the AF scheme can only achieve a small fraction of the G-SDoF. For this system without any CSIT, the total outage event, defined as either connection outage or secrecy outage, is introduced. Based on this total outage definition, analysis shows that the proposed MF scheme achieves the full generalized secure diversity gain (G-SDG) of order one. On the other hand, the AF scheme can only achieve a G-SDG of $1/2$ at most.

S. Zhang is with the School of Information Engineering, Shenzhen University, Shenzhen, China (e-mail: zsl@szu.edu.cn), and also with the Electrical Engineering Department, Stanford CA, USA. L. Fan is with the Department of Electronic Engineering, Shantou University, Shantou, China (e-mail: lsfan@stu.edu.cn). M. Peng is with the Beijing University of Posts & Telecommunications, Beijing, China(e-mail: pmg@bupt.edu.cn), and also with the School of Engineering and Applied Science, Princeton University, Princeton, NJ, USA. H. V. Poor is with the School of Engineering and Applied Science, Princeton University, Princeton, NJ, USA (e-mail: poor@princeton.edu). This research was partially supported in part by the U. S. National Science Foundation under Grant CMMI-1435778.

I. Introduction

The broadcast nature of wireless transmission creates significant security concerns, and physical layer techniques can be used in part to address these concerns. The theoretical basis for physical-layer security can be traced back to Shannon's work on perfect secrecy [1], and to subsequent work by Wyner [2], Leung et al. [3], and others on the wire-tap channel. The basic idea of physical-layer security is to exploit the destination's advantages (e.g, better channel quality) over the eavesdropper. More recent works have investigated this problem in fading channels, including analyses of the fading secrecy capacity [4], [5] and the secrecy outage probability [6], [7]. On the other hand, new coding and modulation schemes have been proposed to achieve physical-layer security, including Low Density Parity Check (LDPC) codes in [8] and [9], nested lattice codes in [10] and [11], and nested polar codes in [12] and [13].

In recent years, several extended models of the wire-tap channel have been studied and one of these is the untrusted relay channel. In the untrusted relay channel, the source relies on a relay node to forward information to the destination, while keeping the transmitted information confidential from the relay. An example is the two-way untrusted relay channel with two-phase physical-layer network coding [14], in which the superimposed signals at the relay protect each other's information with minimal rate loss compared to capacity [15], [16]. Similar ideas have been applied in the one-way untrusted relay channel in which the destination artificially transmits some interference to the relay while the source is transmitting. Depending on the processing at the relay, such schemes can be classified into two categories. The first category is amplify-and-forward (AF), in which the relay simply amplifies the received signal under its power constraint and then forwards it to the destination [17]–[19]. Although AF is simple to implement, its performance is severely limited by the interference power dilemma: more power of the relay is wasted on forwarding the interfering signal (which is useless to the destination) when the destination transmits with larger power to protect the confidential message; alternatively the confidential message is less well protected when the destination transmits with smaller power. The other category is decode-and-forward (DF) [20], in which both source signal and interference signal are encoded by lattice codes and arrive at the relay in perfect synchrony[1], followed by channel decoding to obtain the noiseless network code produced by this signal. The DF scheme

[1]Perfect synchronization here refers to the synchronization of signal amplitude, carrier frequency and carrier phase.

performs better than the AF scheme in the high SNR region but performs worse in the low SNR region, despite the cost of perfect synchronization. Schemes extending these ideas to multiple channels and fading channels can be found in many works, such as [21] and [22].

To counter the shortcomings of these existing techniques and inspired by the modulo-lattice additive noise (MLAN) channel [23] in which modulo processing at the receiver loses very little information, here we propose a novel modulo-and-forward (MF) scheme at the relay. In this scheme, the confidential message from the source node is encoded with a nested lattice code [10] while the artificial interference message from the destination is Gaussian. When the two messages arrive at the relay node simultaneously, the relay maps the superimposed signal to a new signal with a modulo operation according to the source lattice. As a result, the total power of the new message is reduced to that of the source lattice, with almost no loss of useful information. In this way, the proposed MF scheme solves the interference power dilemma of the AF scheme by relaying a signal with only the source power, without relation to the interference power. Moreover, MF does not require perfect synchronization as in the DF scheme.

We analyze the secure performance of this MF scheme for two different cases. For Gaussian channels with full channel state information at the transmitter (CSIT), our analysis shows that the MF scheme approaches the secrecy capacity of the untrusted relay channel within 1/2 bit for all channel realizations; hence it achieves the full generalized secure degrees of freedom (G-SDoF), while the AF scheme can achieve only a small fraction of the G-SDoF. The achievable secrecy rate of MF is also better than that of DF, which as noted above requires fine synchronization.

For fading channels without any CSIT, we characterize the total outage probability, which includes the connection outage probability at the destination and the secrecy outage probability at the relay node [7]. Beyond achieving a smaller outage probability as expected, the MF scheme achieves essential improvement over the AF scheme. Defining the generalized secure diversity as the rate with which the total outage probability goes to zero in the high SNR region, our analysis shows that the MF scheme achieves full diversity gain of 1 as long as the ratio of the destination signal power to the source signal power goes to infinity. The AF scheme, however, can only achieve a diversity gain of 1/2 at most, due to the interference power dilemma.

The contributions of this paper are as follows.

1) **The MF Scheme:** We propose the lattice code based modulo-and-forward scheme for the untrusted relay channel. This scheme is of practical interest since it only needs symbol level

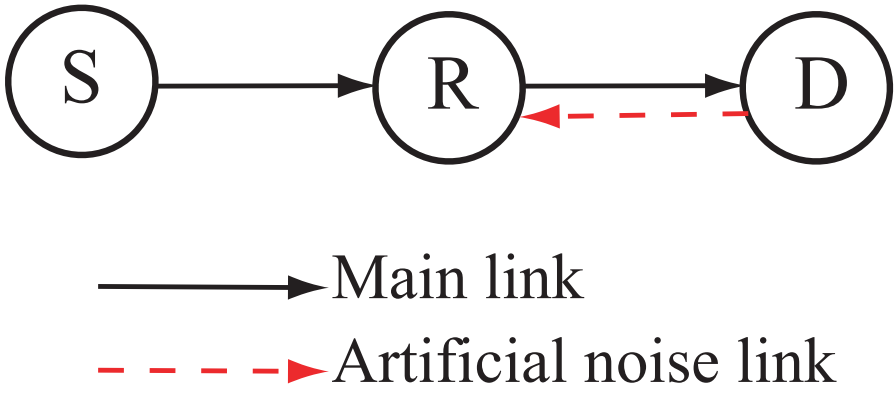

Fig. 1. System model for the untrusted relay channel based on lattice coding.

time synchronization and low complexity processing to obtain much better performance than other schemes.

2) **Analysis of the Secure Capacity and G-SDoF in Gaussian Channels:** In Gaussian channels with full CSIT, we prove that the MF scheme approaches the secrecy capacity within one-half bit for any channel realization. Hence, the MF scheme achieves the full G-SDoF, while the AF scheme only achieves a very small fraction of the G-SDoF.
3) **Analysis of the Secure Diversity in Fading Channels:** In fading channels without CSIT, the MF scheme achieves the full generalized secure diversity gain (G-SDG) value of 1, while the AF scheme only achieves a G-SDG of 1/2 due to the interference power dilemma.

The remainder of this paper is organized as follows. Section II presents the detailed untrusted relay model and the notation used therein. For the proposed modulo-and-forward scheme, Section III elaborates the encoding process at the source node, the forwarding process at the relay node and the decoding process at the destination node. Under the assumption of full CSIT, Section IV analyzes the achievable rate and the G-SDoF of the MF scheme, with a comparison to the AF and DF schemes. Under the assumption of no CSIT, Section V analyzes the connection outage and secrecy outage probabilities, as well as the system secure diversity gain. Finally, Section VI concludes the paper.

II. System Model

Fig. 1 shows the system model for the considered untrusted relay channel, where the source S needs to transmit a confidential message to the destination D with R working as a relay. All nodes are equipped with single antennas, and operate in a time-division half-duplex mode. In this setting, although the source relies on the relay to forward the message, it does not trust the relay and would like to keep the confidential information secret from the relay. This model can find application in many practical scenarios such as renting a satellite from a third party to relay confidential messages.

To prevent eavesdropping at R, an artificial interference scheme is proposed. Specifically, the destination D sends a signal to interfere with reception at the relay, while the source is transmitting to the relay. Then, the relay sends the corrupted source signal to the destination, where it can be recovered since the destination has full information about the interfering signal. This two phase transmission is similar to physical layer network coding as described in [14]. The data transmission process is detailed as follows.

Before transmitting the signal, the source needs to encode its information with a secure encoding scheme, such as those described in [2], [10] and [12]. Essentially, all the schemes can be described as follows. First, the length-L_1 binary confidential message v is combined with a random sequence and mapped to a new binary source message w of length $L_2 \geq L_1$. This is a one-to-one mapping, the rule for which is known to all nodes, although the random sequence itself is not known to either R or D. The sequence w is then channel encoded to a length-N message x_s to combat the channel degradation at the destination.

After secure encoding at the source, the data transmission will operate in two phases as shown in Fig. 1. Specifically, the first phase is a multiple access transmission, in which the source S transmits x_s with power P_s to the relay, and at the same time, D transmits a Gaussian interference signal x_d with power P_d. Hence the relay receives a superimposed signal

$$y_r = h_1 x_s + h_2 x_d + n_r, \tag{1}$$

where $h_i \sim \mathcal{CN}(0, \varepsilon_i)$ denotes the instantaneous channel coefficient of the i-th hop ($i = 1, 2$) in the multiple access phase, and $n_r \sim \mathcal{CN}(0, \sigma^2)$ is additive white Gaussian noise at the relay.

Recall that the relay is untrusted, and we hope to keep the confidential information secret from the relay. Therefore, the relay must not be able to correctly decode w from y_r. On the

other hand, the relay is willing to forward the message to the destination. So it will process y_r to make the transmission to D more efficient. We denote the message sent from the relay by x_r, with the same average power constraint ${P_s}^2$.

The second phase is a point-to-point forwarding transmission, where R transmits x_r to the destination D. As a result, the received signal at D can be expressed as

$$y_d = h_2 x_r + n_d, \tag{2}$$

where $n_d \sim \mathcal{CN}(0, \sigma^2)$ is additive white Gaussian noise at the destination and the corresponding channel coefficient is also h_2 under the assumption of reciprocity.

Let $g_i = |h_i|^2$ be the instantaneous channel gain of the i-th hop ($i \in \{1, 2\}$). For an amplify-and-forward relay scheme, $x_r = \tau y_r$ with the normalizing coefficient $\tau = \sqrt{\frac{P_s}{P_s g_1 + P_d g_2 + \sigma^2}}$. Although the artificial interference x_d protects the confidential message from eavesdropping at R, it also degrades the performance of the useful information at the destination since it decreases the normalizing coefficient τ via the term P_d therein. Better protection with larger P_d also consumes more power at the relay, which is the interference power dilemma, as noted above. To solve this dilemma, i.e., to overcome the detrimental effects of the artificial interference and keep its beneficial effects at the same time, we now propose a modulo-and-forward scheme as detailed in the next section.

III. Modulo-and-Forward Scheme

In the amplify-and-forward scheme, a good part of the relay's power is used to convey the interference, which is totally useless for the destination D. To counter this problem, we propose a modulo-and-forward scheme, in which the relay processes y_r with a modulo operation before forwarding it. This scheme is detailed as follows.

A. Lattice Encoding at S

We consider the nested lattice coding scheme of [10]. Let $(\Lambda, \Lambda_0, \Lambda_1)$ be properly designed nested lattices such that $\Lambda_1 \subset \Lambda_0 \subset \Lambda$, and their associated fundamental Voronoi regions are denoted by $\mathcal{V}_1, \mathcal{V}_0,$ and $\mathcal{V}$, respectively. The Voronoi regions are selected such that the average

[2] There is no loss of generality with this assumption since the transmit power can be combined into the channel coefficient in the second phase.

power of points in $\mathcal{V}_1$ is P_s. All points in $(\Lambda, \Lambda_0, \Lambda_1)$ are length-L vectors. We define the codebook $\mathcal{C} = \{\Lambda \cap \mathcal{V}_0\}$ and there is a one-to-one mapping between each codeword in $\mathcal{C}$ and each confidential message v. Therefore, the cardinality of $\mathcal{C}$ is $|\mathcal{C}| = 2^{L_1}$. We then define another codebook $\mathcal{C}' = \{\Lambda_0 \cap \mathcal{V}_1\}$ and the cardinality of this codebook is $|\mathcal{C}'| = 2^{L_2 - L_1}$. Therefore, there is a one-to-one mapping between any codeword in $\mathcal{C}'$ and any length-$(L_2 - L_1)$ binary sequence.

For any message v, the source selects the corresponding codeword c_m in $\mathcal{C}$, and then it generates a random bit sequence of length $L_2 - L_1$, which is mapped to one codeword b_m in $\mathcal{C}'$. Before transmission, the source S calculates the nested lattice codeword as $x_s = (c_m + b_m + u) \mod \Lambda_1$, equal to $(a_m + u) \mod \Lambda_1$, where u is a dither vector uniformly distributed over $\mathcal{V}_1$ and $a_m = (c_m + b_m) \mod \Lambda_1$. Obviously, the average power of x_s is still P_s.

B. Modulo Operation at R

After the first phase transmission, the relay R receives $y_r = h_1 x_s + h_2 x_d + n_r$. Instead of forwarding y_r directly as in the AF scheme, the relay scales the received signal[3] and reduces it modulo Λ_1, i.e.,

$$\begin{aligned} x_r &= [\beta \frac{1}{h_1} y_r + u_1] \text{ mod } \Lambda_1 \\ &= [\beta(x_s + h_2/h_1 x_d + n_r/h_1) + u_1] \text{ mod } \Lambda_1, \end{aligned} \tag{3}$$

where u_1 is a random dither vector uniformly distributed over $\mathcal{V}_1$ and is known by all the nodes, and β is chosen as $\frac{P_s}{P_s + \sigma^2/g_1}$ to minimize interference at the destination as explained later.

According to the lemma in [23], x_r is also uniformly distributed over $\mathcal{V}_1$ and its average power is P_s. As it is assumed that the relay has the same transmit power constraint as P_s, it can directly forward the resulting signal x_r to the destination D.

C. Lattice Decoding at D

After receiving the signal y_d of (2), the destination D exploits inflated lattice decoding [23]. Specifically, D multiplies the received signal by a coefficient α, and then cancels both the

[3]With equalization at the relay, our modulo-and-forward scheme can be applied to both the in-phase and quadrature phase signals. For simplicity, we focus only on the in-phase signal processing here.

self-interference x_d and the dither vector u, u_1 as

$$y = \Big(\frac{\alpha}{h_2} y_d - \beta \frac{h_2}{h_1} x_d - u - u_1\Big) \bmod \Lambda_1, \tag{4}$$

where α and β are scaling factors to be selected to minimize the power of the residual interference plus noise. By substituting (2) and (3) into (4) and applying processing similar to that in [23] and [24], we can write y as

$$\begin{aligned} y &= \Big(\alpha(x_r + \frac{n_d}{h_2}) - \beta \frac{h_2}{h_1} x_d - u - u_1\Big) \bmod \Lambda_1 \\ &= \Big(x_r + (\alpha - 1)x_r + \alpha \frac{n_d}{h_2} - \beta \frac{h_2}{h_1} x_d - u - u_1\Big) \bmod \Lambda_1 \\ &= \Big(\beta x_s + \beta \frac{n_r}{h_1} + (\alpha - 1)x_r + \alpha \frac{n_d}{h_2} - u\Big) \bmod \Lambda_1 \\ &= \Big(x_s + (\beta - 1)x_s + \beta \frac{n_r}{h_1} + (\alpha - 1)x_r + \alpha \frac{n_d}{h_2} - u\Big) \bmod \Lambda_1 \\ &= \Big(a_m + (\alpha - 1)x_r + (\beta - 1)x_s + \beta \frac{n_r}{h_1} + \alpha \frac{n_d}{h_2}\Big) \bmod \Lambda_1, \end{aligned} \tag{5}$$

where the residual interference plus noise becomes $\big((\alpha-1)x_r + (\beta-1)x_s + \beta\frac{n_r}{h_1} + \alpha\frac{n_d}{h_2}\big)$, with an upper bound on the variance of $(1-\alpha)^2 P_s + (1-\beta)^2 P_s + \alpha^2\sigma^2/g_2 + \beta^2\sigma^2/g_1$. We then select α and β to minimize this upper bound on the variance[4]. It is easy to see that the optimal values of the scaling factors are $\alpha = \frac{P_s}{P_s + \sigma^2/g_2}$ and $\beta = \frac{P_s}{P_s + \sigma^2/g_1}$. As a result, the equivalent noise variance of the post-modulo signal at D becomes

$$\sigma_e^2 = \min\Big\{P_s, \frac{P_s\sigma^2}{g_1 P_s + \sigma^2} + \frac{P_s\sigma^2}{g_2 P_s + \sigma^2}\Big\}, \tag{6}$$

and we ignore the case of $\sigma_e^2 = P_s$ hereafter for simplicity.

Then, the decoder at the destination can use Euclidean lattice decoding to decode a_m as

$$\hat{a}_m = \mathcal{Q}_{\mathcal{V}}(y) \bmod \Lambda_1, \tag{7}$$

where $\mathcal{Q}_{\mathcal{V}}(x)$ is the nearest neighbor quantizer defined as $\mathcal{Q}_{\mathcal{V}}(x) = \arg\min_{a\in\Lambda} ||x - a||$. $\hat{a}_m$ can then be mapped to an estimate of w directly (note that w includes both information of confidential message v and the random generated information.).

As proved in [23], the error probability $\Pr(a_m \neq \hat{a}_m)$ goes to zero as long as the total transmission rate $R_d = L_2/L$ is less than the direct channel capacity $C_d = \frac{1}{2}\log(P_s/\sigma_e^2)$. We

[4] x_r, x_s and a_m are independent of each other with the random dither vector u and u_1 as in [23].

use $C_r = \frac{1}{2}\log(1 + g_1 P_s/(g_2 P_d + \sigma^2))$ to denote the channel capacity for the untrusted relay (with interference). As proved in [10], this nested scheme can guarantee that the untrusted relay obtains no information about the confidential message as long as the confidential rate $R_s = L_1/L$ is less than the secrecy capacity $[C_d - C_r]^+$, where $[x]^+ = \max(0, x)$.

By decreasing the power of the effective signal y_r/h_1 from $P_s + \frac{g_2}{g_1}P_d + \frac{\sigma^2}{g_1}$ to P_s, the MF scheme can substantially improve the performance of the untrusted relay channel. The performance of MF is analyzed in the next two sections.

IV. Secrecy Capacity Analysis with Full CSIT

In this section, we analyze the capacity performance on the untrusted relay channel, in terms of the secrecy capacity and the generalized secure degrees of freedom, under the assumption of full CSIT. This section consists of four parts: Part A presents the definition of secrecy rate and generalized secure degrees of freedom; Part B presents upper bounds for the secrecy rate and G-SDoF for any forwarding protocol; Part C calculates the achievable secrecy rate and G-SDoF of the MF scheme; and finally Part D provides a comparison with the AF and DF forwarding schemes.

A. Secrecy Rate and G-SDoF

When the channel varies slowly and the channel information can be fed back to the transmitter, all the channel information can be pre-known by the transmitter. In this case, the transmitter can carefully select the confidential message rate R_s and the mixed message rate R_d respectively, such that the confidential message is correctly and securely transmitted to the destination at the maximal rate. In this case, the achievable secrecy capacity region has been derived in [2] and is given by

$$R_s \le R_d \le C_d \quad 0 \le R_s \le [C_d - C_r]^+, \tag{8}$$

where C_d and C_r are the channel capacities from the source to the destination (via the relay) and the channel capacity from source to the relay, respectively. In this case, therefore, the secrecy capacity is the most important factor indicating the system performance.

In the high SNR region, degrees of freedom is a good metric to analyze the system rate performance. Analogous to the generalized degrees of freedom definition in [25], we further

define the generalized secure degrees of freedom as

$$SD(\rho) = \limsup_{SNR\to\infty} \frac{R_s(SNR,\rho)}{\log(SNR)}, \tag{9}$$

where SNR is defined as P_s/σ^2 and $\rho = \log(INR)/\log(SNR)$, with $INR = P_d/\sigma^2$ being the interference-to-noise ratio.

B. Upper Bound on Secrecy Rate and G-SDoF

We firstly present an upper bound on the secrecy rate for any possible forwarding protocol and processing at the relay node. As proved in [2] and [3], the secrecy rate for a wiretap channel is upper bounded by $[C_d - C_r]^+$. In our system, the destination channel capacity C_d is upper bounded by the minimum capacity of the two-hop channel based on the cut-set bound, which is $C_d \leq \frac{1}{2}\log(1+\min\{g_1,g_2\}\frac{P_s}{\sigma^2})$. On the other hand, the capacity of the relay channel, $C_r = \frac{1}{2}\log(1+\frac{g_1P_s}{g_2P_d+\sigma^2})$, is achievable with properly selected lattices. As a result, an upper bound on the secrecy rate for this two-hop channel is given by

$$U = \left[\frac{1}{2}\log\left(1+\min\{g_1,g_2\}\frac{P_s}{\sigma^2}\right) - \frac{1}{2}\log(1+\frac{g_1P_s}{g_2P_d+\sigma^2})\right]^+. \tag{10}$$

We secondly present an upper bound for the G-SDoF. Substituting the upper bound in (10) to the definition in (9), we can easily obtain an upper bound on the G-SDoF as

$$\begin{aligned} SD_u(\rho) &= \limsup_{SNR\to\infty} \frac{\frac{1}{2}\log(1+\min\{g_1,g_2\}\frac{P_s}{\sigma^2}) - \frac{1}{2}\log(1+\frac{g_1P_s}{g_2P_d+\sigma^2})}{\log(SNR)} \\ &= \frac{1}{2}\limsup_{SNR\to\infty} \frac{\log\left(SNR\min(g_1,g_2)\right) - \log\left(1+\frac{g_1SNR}{g_2INR}\right)}{\log(SNR)} \\ &= \frac{1}{2}\limsup_{SNR\to\infty} \left[1 - \frac{\log\left(1+\frac{g_1}{g_2}SNR^{1-\rho}\right)}{\log(SNR)}\right] \\ &= \begin{cases} \rho/2, & \text{If } 0\leq\rho<1 \\ 1/2, & \text{If } 1\leq\rho \end{cases}. \end{aligned} \tag{11}$$

The G-SDoF must be no more than the generalized degrees of freedom without a security constraint, which is at most 1/2 in our two-hop single antenna system due to the two-phase transmission. And this best secure DoF may be achieved when the transmission power of the destination is no less than that of the source, as shown in (11).

C. Achievable Secrecy Rate and G-SDoF with MF

We now calculate the achievable secrecy rate and G-SDoF for the modulo-and-forward scheme.

1) Achievable Secrecy Rate: With reference to (6), a good nested lattice code can achieve the following rate to the destination:

$$\begin{aligned} R_d &= \frac{1}{2}\log\Big(\frac{P_s}{\sigma_e^2}\Big) \\ &= \frac{1}{2}\log\Big(\frac{1}{\frac{\sigma^2}{g_1P_s+\sigma^2}+\frac{\sigma^2}{g_2P_s+\sigma^2}}\Big) \\ &\geq \frac{1}{2}\log\Big(\frac{1}{2}+\frac{P_s}{\sigma^2}\frac{g_1g_2}{g_1+g_2}\Big). \end{aligned} \tag{12}$$

From (1), we can compute the maximum information obtained by the relay. With the assumption that the relay knows all the nested lattice codebook information and the channel state information to detect the combined information w, the maximal information rate is

$$R_r = \frac{1}{2}\log\Big(1+\frac{P_sg_1}{P_dg_2+\sigma^2}\Big). \tag{13}$$

Then, the achievable secrecy rate of the proposed modulo-and-forward scheme is given by

$$R_s \geq \frac{1}{2}\left[\log\Big(\frac{1}{2}+\frac{P_s}{\sigma^2}\frac{g_1g_2}{g_1+g_2}\Big)-\log\Big(1+\frac{P_sg_1}{P_dg_2+\sigma^2}\Big)\right]^+. \tag{14}$$

From (14), we can see that the artificial noise power P_d only helps to improve the secrecy rate with almost no detrimental effect on the transmission from S to D in our modulo-and-forward scheme. When P_d goes to infinity, R_s can approach the upper bound of $\frac{1}{2}\log\Big(1/2+\frac{P_s}{\sigma^2}\frac{g_1g_2}{g_1+g_2}\Big)$. Therefore, the MF scheme solves the interference power dilemma of the AF scheme.

We now calculate the gap between the upper bound and the achievable rate in the non-trivial regime, i.e., $U>0$ and $R_s>0$. Without loss of generality, we assume that $g_1 \leq g_2$. Then, we obtain the gap as

$$U-R_s \leq \frac{1}{2}\log\Big(1+\frac{g_1+g_2+2g_1^2P_s/\sigma^2}{g_1+g_2+2g_1g_2P_s/\sigma^2}\Big) \leq 1/2, \tag{15}$$

which goes to zero as g_1/g_2 goes to zero in the high SNR region. In other words, when the ratio between the two-hop channel gains, g_1 and g_2, becomes very large or small, the achievable rate of the modulo-and-forward scheme approaches the upper bound for small noise variance. In summary, we have the following theorem,

Theorem 1: The modulo-and-forward scheme achieves a secrecy rate R_s of (14), which is within one-half bit of the secrecy capacity for all channel realizations[5].

2) Achievable G-SDoF: Now we characterize the G-SDoF of the MF scheme. Substituting (14) into the definition of G-SDoF in (9), we have

$$\begin{aligned} SD_{mf}(\rho) &\geq \limsup_{SNR\to\infty} \frac{\frac{1}{2}\log\left(1/2+\frac{P_s}{\sigma^2}\frac{g_1g_2}{g_1+g_2}\right)-\frac{1}{2}\log\left(1+\frac{P_sg_1}{P_dg_2+\sigma^2}\right)}{\log(SNR)} \\ &= \frac{1}{2}\limsup_{SNR\to\infty} \frac{\log\left(SNR\frac{g_1g_2}{g_1+g_2}\right)-\log\left(1+\frac{SNRg_1}{INRg_2}\right)}{\log(SNR)} \\ &= \frac{1}{2}\limsup_{SNR\to\infty} 1-\frac{\log\left(1+\frac{g_1}{g_2}SNR^{1-\rho}\right)}{\log(SNR)} \\ &= \begin{cases} \rho/2, & \text{If } 0\leq\rho<1 \\ 1/2, & \text{If } 1\leq\rho \end{cases}. \end{aligned} \tag{16}$$

As an upper bound on G-SDoF, $SD_u(\rho) \geq SD_{mf}(\rho)$ holds. On the other hand, $SD_{mf}(\rho) \geq SD_u(\rho)$ is obtained from the equation above. Hence we can conclude that $SD_{mf}(\rho) = SD_u(\rho)$ exactly. Thus, we have the following theorem,

Theorem 2: The modulo-and-forward scheme achieves the full generalized secrecy degrees of freedom for the untrusted relay channel.

D. Comparison with AF and DF Schemes

This subsection compares the MF scheme with the AF scheme in terms of secrecy rate and the generalized secure degrees of freedom.

1) Secrecy Rate Comparison with AF: For the AF scheme, the relay node will amplify the received signal in (1) with a coefficient $\tau = \sqrt{P_s/(g_1P_s+g_2P_d+\sigma^2)}$ before sending it to the destination D. As a result, the destination receives the signal

$$\begin{aligned} y_d' &= \tau h_2 y_r + n_d \\ &= \tau h_1 h_2 x_s + \tau h_2^2 x_d + \tau h_2 n_r + n_d. \end{aligned} \tag{17}$$

[5] The above analysis ignores the case that $U > 0$ and $R_s < 0$. In fact, it is easy to verify that $U < 1/2$ when $R_s < 0$. Therefore, this theorem is true for all channel realizations.

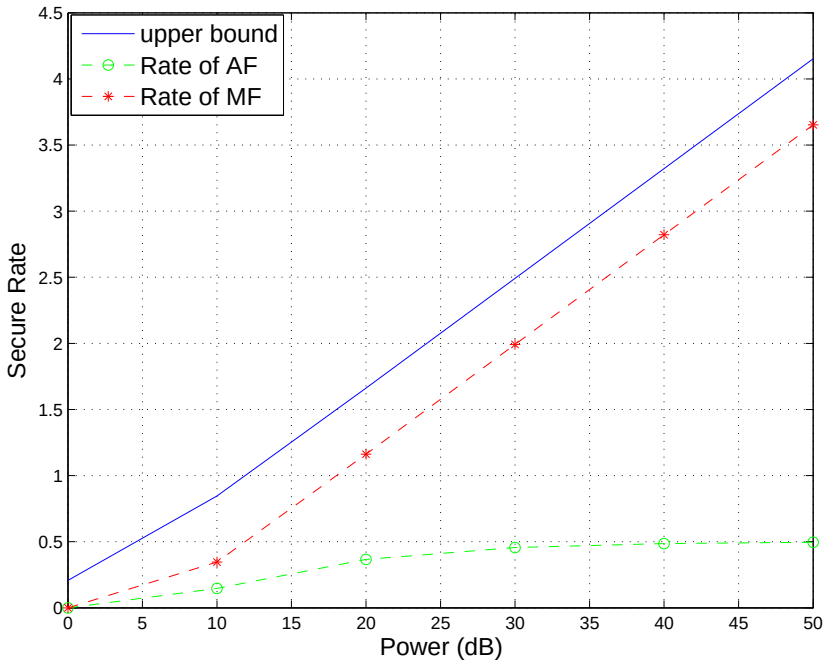

Fig. 2. Secrecy rate versus P_d, where $P_s = \sqrt{P_d}$ and $\sigma^2 = 1$.

Since the destination has full knowledge of x_d and the channel coefficients, it can completely remove the self-interference term $\tau h_2^2 x_d$, and the resulting SNR of the target signal becomes

$$SNR_{AF} = \frac{P_s^2 g_1 g_2}{\sigma^2[P_s g_1 + P_s g_2 + P_d g_2 + \sigma^2]}. \tag{18}$$

Then, we can calculate the secrecy rate of the traditional AF scheme as [26]

$$R_{af} = \left[\frac{1}{2}\log\left(1 + \frac{P_s^2 g_1 g_2}{\sigma^2[P_s g_1 + P_s g_2 + P_d g_2 + \sigma^2]}\right) - \frac{1}{2}\log\left(1 + \frac{P_s g_1}{P_d g_2 + \sigma^2}\right)\right]^+. \tag{19}$$

By comparing R_{AF} with R_s in (14), it is easy to verify that the secrecy rate of the MF scheme, R_s, is always larger than that of the traditional AF scheme. Specifically, consider the case in which $\sigma^2 \to 0, P_d \to \infty$, with $P_d * \sigma^2$ and other parameters constant. Then R_{AF} in (19) is a constant while the rate R_s in (14) increases without bound. In other words, the improvement of the MF scheme over the AF scheme can be arbitrarily large.

In Fig. 2, we plot the achievable secrecy rate of the MF and AF schemes, as well as the upper bound in (10) versus transmission power P_d. In particular, we set $g_1 = g_2 = 1$, $P_s = \sqrt{P_d}$ and

$\sigma = 1$. The figure verifies that the rate of the MF scheme and the upper bound increase with the transmission power, and their gap is always less than $1/2$. On the other hand, the rate of the AF scheme approaches a constant of $1/2$.

2) G-SDoF Comparison with AF: Since the rate gap between the MF and the AF schemes can be arbitrarily large in the high SNR region, their G-SDoF should be different. Here, we calculate the G-SDoF of the AF scheme to make a comparison. According to the definition in (9), we can calculate the G-SDoF of the AF scheme as follows:

$$\begin{aligned} SD_{af}(\rho) &= \limsup_{SNR\to\infty} \frac{\frac{1}{2}\log\left(1+\frac{P_s^2 g_1 g_2}{\sigma^2[P_s g_1+P_s g_2+P_d g_2+\sigma^2]}\right)-\frac{1}{2}\log\left(1+\frac{P_s g_1}{P_d g_2+\sigma^2}\right)}{\log(SNR)} \\ &= \frac{1}{2}\limsup_{SNR\to\infty} \frac{\log\left(1+SNR\frac{SNR g_1 g_2}{SNR(g_1+g_2)+INR g_2}\right)-\log\left(1+\frac{SNR g_1}{INR g_2}\right)}{\log(SNR)} \\ &= \frac{1}{2}\limsup_{SNR\to\infty} \frac{\log\left(1+SNR^{2-\rho}\frac{g_1 g_2}{SNR^{1-\rho}(g_1+g_2)+g_2}\right)-\log\left(1+\frac{g_1}{g_2}SNR^{1-\rho}\right)}{\log(SNR)} \\ &= \begin{cases} \rho/2, & \text{If } 0\le\rho<1 \\ 1-\rho/2, & \text{If } 1\le\rho<2 \\ 0, & \text{If } 2\le\rho \end{cases} . \end{aligned} \tag{20}$$

We plot the G-SDoF of AF and MF in Fig. 3 for an intuitive comparison. With reference to (19), its first term, $\frac{1}{2}\log\left(1+\frac{P_s^2 g_1 g_2}{\sigma^2[P_s g_1+P_s g_2+P_d g_2+\sigma^2]}\right)$, is a decreasing function of P_d while the second term, $-\frac{1}{2}\log\left(1+\frac{P_s g_1}{P_d g_2+\sigma^2}\right)$, is an increasing function of P_d. Hence, the destination needs to carefully select an optimal value of P_d to maximize the rate R_{af} if all the channel information is also available at the destination (this is the interference power dilemma). In the high SNR regime, P_d is easier to calculate with reference to (20), i.e., P_d and P_s should have the same order ($\rho = 1$).

3) Comparison with DF: In the AF and MF schemes, only symbol level time synchronization is required at the multiple access phase. Currently, there is no capacity approaching DF scheme under this assumption. In this part, we compare the MF scheme with the lattice based DF scheme in [20], where perfect phase, amplitude and time synchronization between the interfering signal and the source signal are assumed.

With reference to [20], setting $h_1 = h_2$, and $P_s = P_d$, the achievable rate of lattice DF scheme

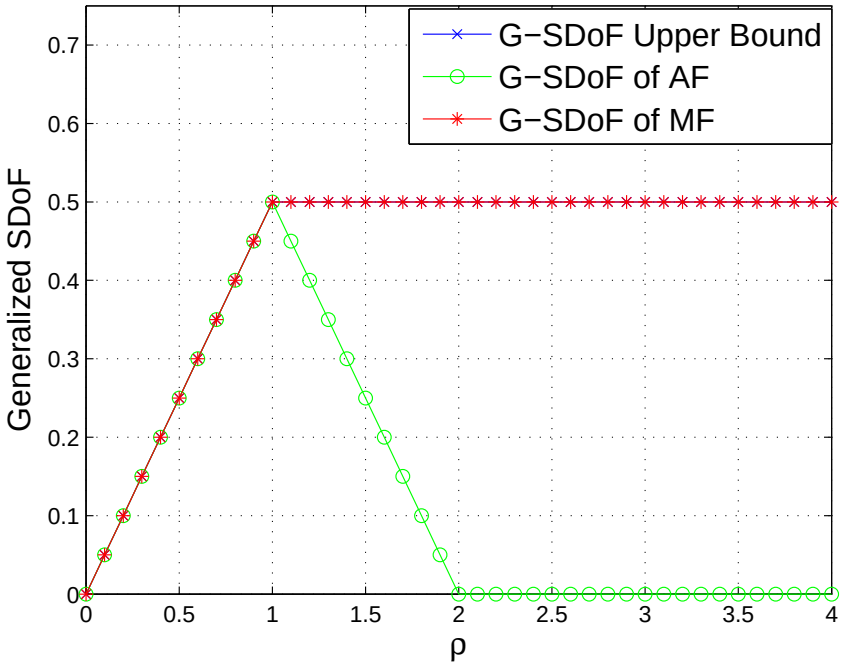

Fig. 3. Generalized secure degrees of freedom versus ρ .

is

$$R_{df} = \frac{1}{2}\log\left(\frac{1}{2} + \frac{P_s g_1}{\sigma^2}\right) - 1.$$

With the same channel coefficients, the MF scheme can also achieve a larger secure rate even without such a strict synchronization requirement. The secrecy rate improvement can be calculated as

$$R_s - R_{df} = \begin{cases} 0 & \text{If } t \leq 1 \\ \frac{1}{2}\log(1+t) - \frac{1}{2} & \text{If } 1 < t \leq 3/2 \\ \frac{1}{2}\log\left(2 + \frac{2}{1+2t}\right) & \text{If } t > 3/2 \end{cases}, \tag{21}$$

where $t = P_s g_1/\sigma^2$ is the receiver side SNR. From (21), we can see that the gap will always be larger than 0 for the non-trivial case. For the low SNR region, the improvement of the MF

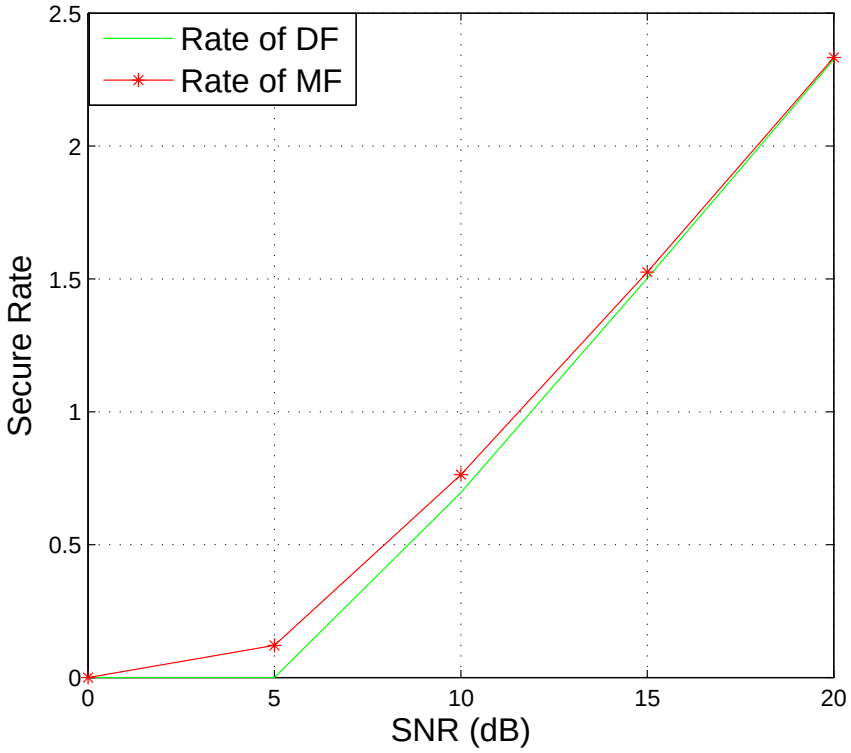

Fig. 4. Secure capacity versus $SNR = P_s g_1/\sigma^2$.

scheme could be significant since R_s/R_{df} can goes to infinity[6].

V. Outage Performance without CSIT

In this section, we analyze the connection outage and secrecy outage performance of the MF scheme under the assumption of only receiver side channel state information. Specifically, this section consists of four parts: Part A presents the formulation of connection and secrecy outage probabilities, as well as the generalized secure diversity; Parts B and C calculate a lower bound and the achievable probability for the outage probabilities, as well as the secure diversity; and Part D provides a comparison with the AF scheme.

[6]The achievable rate in [20] may be further improved with a better bounding technique. However, the MF scheme should outperform it at least in the low SNR region.

A. Outage Probabilities and Diversity

The metrics of secrecy capacity and secrecy outage have been widely investigated to measure the performance of various schemes. However, they are not appropriate when the transmitter has no channel state information. In many cases, such as the fast fading case [27], even the state information of the source-destination channel is difficult to obtain at the transmitter. Of course, with an untrusted channel state information provider, such as the relay in our system model, other issues arise.

Without any CSIT, both the direct channel rate R_d and the secrecy rate R_s must be determined before transmission. Thus, there is always the possibility of unsuccessful transmissions. There are of two types of unsuccessful transmissions to consider: (1) secrecy outage, in which the eavesdropper obtains some information about the confidential message; and (2) connection outage, in which the destination fails to detect the mixed and confidential messages. We use the C-S outage (connection outage and secrecy outage) probability to measure the system secure performance [7]. We formulate the C-S performance as follows.

1) Outage Probabilities Formulation: To discuss the outage probabilities, we define three events: (1) E_A: secrecy outage occurs at the relay and no connection outage occurs at the destination; (2) E_B: connection outage occurs at the destination and no secrecy outage occurs at the relay; and (3) E_C: both connection outage and secrecy outage occur.

A connection outage event occurs when the receiver cannot correctly decode the received message. The connection outage probability can be written as

$$p_{c,out} = \Pr(E_B \cup E_C) = \Pr(C_d < R_d). \tag{22}$$

A secrecy outage event occurs when the eavesdropper can obtain some information about the confidential message. This event happens when the total information the eavesdropper can retrieve from the received message is more than the entropy of the random sequence. So, the secrecy outage probability can be written as

$$p_{s,out} = \Pr(E_A \cup E_C) = \Pr(R_d - R_s < C_r) = \Pr(R_s > R_d - C_r). \tag{23}$$

Both $p_{c,out}$ and $p_{s,out}$ are of interest in this paper since the connection outage and secrecy outage may be of different severities in various scenarios. For a given R_s, there is a tradeoff between the connection outage probability and secrecy outage probability, since a large R_d will

decrease the secrecy outage probability while increasing the connection outage probability, and vice versa.

2) Definition of G-SDG: In the high SNR region, diversity order is a simple metric to characterize the system performance. We now define the generalized secure diversity gain. Similar to the generalized diversity gain defined in [28], the G-SDG is defined as

$$DG(\rho) = \limsup_{SNR\to\infty} \frac{-\log p_t(SNR,\rho)}{\log(SNR)} \tag{24}$$

where $SNR = P_s/\sigma^2$, an exact expression for $\rho = \log(INR)/\log(SNR)$ are defined the same as for the G-SDoF in (9), and p_t is the total outage probability $p_t = \Pr(E_A)+\Pr(E_B)+\Pr(E_C)$.

B. Bounds on Outage Probabilities and Diversity Orders

This section develops a lower bound on the connection outage probability, an expression for the secrecy outage probability, and an upper bound on the G-SDG, for any possible processing at the relay node.

1) Lower Bound on Connection Outage: With reference to the definition in (22), a lower bound on the connection outage probability can be obtained when the direct channel capacity C_d is replaced with its upper bound $\frac{1}{2}\log(1+\min\{g_1,g_2\}P_s/\sigma^2)$. Then, we have a lower bound on the connection outage probability as

$$p_{c,out}^{lb} = \Pr\left(\frac{1}{2}\log(1+\min\{g_1,g_2\}P_s/\sigma^2) < R_d\right) \tag{25}$$

$$= \Pr\left(\min\{g_1,g_2\}P_s/\sigma^2 < \gamma_o\right), \tag{26}$$

where $\gamma_o = 2^{2R_d}-1$ is the SNR threshold associated with connection outage. We further derive $p_{c,out}^{lb}$ as

$$p_{c,out}^{lb} = 1 - \Pr\left(\min\{g_1,g_2\}P_s/\sigma^2 \geq \gamma_o\right) \tag{27}$$

$$= 1 - \Pr\left(g_1 \geq \frac{\gamma_o\sigma^2}{P_s}\right)\Pr\left(g_2 \geq \frac{\gamma_o\sigma^2}{P_s}\right) \tag{28}$$

$$= 1 - e^{-(\frac{1}{\varepsilon 1}+\frac{1}{\varepsilon 2})\frac{\gamma_o\sigma^2}{P_s}}. \tag{29}$$

where the last equation is obtained by noting the probability density functions $f_{g_1}(x) = \frac{1}{\varepsilon_1}e^{-\frac{x}{\varepsilon_1}}$ and $f_{g_2}(x) = \frac{1}{\varepsilon_2}e^{-\frac{x}{\varepsilon_2}}$.

2) Expression for the Secrecy Outage: The secrecy outage does not depend on the processing at the relay node. Therefore, we do not need to provide a bound, but rather can deal with the exact outage probability. With the secrecy outage probability definition in (23), we derive an analytical expression for the secrecy outage probability as follows:

$$\begin{aligned} p_{s,out} &= \Pr\left(C_r > R_d - R_s\right) \\ &= \Pr\Big(\frac{P_s g_1}{P_d g_2 + \sigma^2} > \gamma_s\Big), \end{aligned} \tag{30}$$

where $\gamma_s = 2^{2(R_d - R_s)} - 1$ is the secrecy outage SNR threshold. We further write $p_{s,out}$ as

$$\begin{aligned} p_{s,out} &= \Pr\left(P_s g_1 > \gamma_s P_d g_2 + \gamma_s \sigma^2\right) \\ &= \Pr\Big(g_1 > \frac{\gamma_s P_d}{P_s} g_2 + \frac{\gamma_s \sigma^2}{P_s}\Big) \\ &= \int_0^\infty f_{g_2}(g_2)\Big(\int_{\frac{\gamma_s P_d}{P_s} g_2 + \frac{\gamma_s \sigma^2}{P_s}}^\infty f_{g_1}(g_1) dg_1\Big) dg_2. \end{aligned} \tag{31}$$

Applying the probability density functions $f_{g_1}(x) = \frac{1}{\varepsilon_1} e^{-\frac{x}{\varepsilon_1}}$ and $f_{g_2}(x) = \frac{1}{\varepsilon_2} e^{-\frac{x}{\varepsilon_2}}$ in the above equation, we can obtain an analytical expression of $p_{s,out}$ as follows:

$$\begin{aligned} p_{s,out} &= \frac{1}{\varepsilon_2} e^{-\frac{\gamma_s \sigma^2}{P_s \varepsilon_1}} \int_0^\infty e^{-(\frac{1}{\varepsilon_2} + \frac{\gamma_s P_d}{P_s \varepsilon_1}) g_2} dg_2 \\ &= \frac{P_s \varepsilon_1}{P_s \varepsilon_1 + P_d \varepsilon_2 \gamma_s} e^{-\frac{\gamma_s \sigma^2}{P_s \varepsilon_1}}. \end{aligned} \tag{32}$$

By applying the approximation $e^x = 1 + x$ for small values of $|x|$ again, we arrive at an asymptotic expression for the secrecy outage probability with high transmit power P_s, namely

$$p_{s,out} \simeq \frac{P_s \varepsilon_1}{P_s \varepsilon_1 + P_d \varepsilon_2 \gamma_s} \Big(1 - \frac{\gamma_s \sigma^2}{P_s \varepsilon_1}\Big). \tag{33}$$

3) Upper Bound on G-SDG: According to the definition, an outage event occurs when either a secrecy outage or a connection outage occurs. Therefore, we have a lower bound on the total outage probability:

$$p_t \geq \max\{p_{c,out}^{lb}, p_{s,out}\}. \tag{34}$$

With the generalized secure diversity gain defined in (24), we can then obtain an upper bound on the G-SDG as

$$G\text{-}SDG_{up}(\rho) = \limsup_{SNR\to\infty} \frac{-\log(\max[p_{c,out}^{lb}(SNR,\rho), p_{s,out}(SNR,\rho)])}{\log(SNR)} \tag{35}$$

$$= \limsup_{SNR\to\infty} \frac{-\max[\log p_{c,out}^{lb}(SNR,\rho), \log p_{s,out}(SNR,\rho)]}{\log(SNR)} \tag{36}$$

$$= \limsup_{SNR\to\infty} \frac{\min[-\log((\frac{1}{\varepsilon_1}+\frac{1}{\varepsilon_2})\frac{\gamma_o}{SNR}), -\log(\frac{P_s\varepsilon_1}{P_s\varepsilon_1+P_d\varepsilon_2\gamma_s}(1-\frac{\gamma_s}{SNR\varepsilon_1}))]}{\log(SNR)} \tag{37}$$

$$= \min\Big[1, \limsup_{SNR\to\infty} \frac{-\log(\frac{SNR\varepsilon_1}{SNR\varepsilon_1+SNR^{\rho}\varepsilon_2\gamma_s})}{\log(SNR)}\Big] \tag{38}$$

$$= \begin{cases} 0 & \text{If } \rho \le 1 \\ \rho - 1 & \text{If } 1 < \rho \le 2 \\ 1 & \text{If } \rho > 2 \end{cases}. \tag{39}$$

C. Achievable Outage Probabilities and Diversity

In this section, we first derive the probabilities $p_{c,out}$ and $p_{s,out}$ achievable with the MF scheme, separately. With these probabilities, we then obtain the achievable generalized secure diversity gain of the MF scheme. The achievable $p_{s,out}$ is the same as the expression in (32).

1) Achievable Connection Outage Probability: The achievable connection outage probability can be written as

$$p_{c,out} = \Pr(C_d < R_d)$$

$$= \Pr\Big[\frac{1}{2}\log_2\Big(1/2 + \frac{P_s}{\sigma^2}\frac{g_1 g_2}{g_1+g_2}\Big) < R_d\Big] \tag{40}$$

$$= 1 - e^{-(\frac{1}{\varepsilon_1}+\frac{1}{\varepsilon_2})\frac{\gamma_1\sigma^2}{P_s}} \frac{2\gamma_1\sigma^2}{P_s\sqrt{\varepsilon_1\varepsilon_2}} K_1\Big(\frac{2\gamma_1\sigma^2}{P_s\sqrt{\varepsilon_1\varepsilon_2}}\Big), \tag{41}$$

where $\gamma_1 = \gamma_o - 1/2$ and $K_1(x)$ denotes the first-order modified Bessel function of the second kind, and the derivation from (40) to (41) is given in Appendix I.

By applying the approximation of $K_1(x) \simeq \frac{1}{x}$ and $e^x = 1+x$ for small values of $|x|$, we arrive at an asymptotic expression for the connection outage probability with high transmit power P_s as

$$p_{c,out} \simeq \Big(\frac{1}{\varepsilon_1}+\frac{1}{\varepsilon_2}\Big)\frac{\gamma_1\sigma^2}{P_s}. \tag{42}$$

2) Tradeoff between Achievable $p_{c,out}$ and $p_{s,out}$: With reference to (32) and (41), we see that the two probabilities are not independent. An increase in $p_{c,out}$ ($p_{s,out}$) will lead to a decrease in $p_{s,out}$ ($p_{c,out}$), which is a tradeoff mentioned in [7]. With the given tradeoff, it would be interesting to carefully design the rates R_s, R_d and the powers P_s, P_d to minimize the connection outage and secrecy outage probabilities. In the following Fig. 5, we plot the tradeoff between the connection outage and secrecy outage probabilities for a typical setting.

In the high SNR regime with large P_s/σ^2, the tradeoff between the two probabilities is simpler. Substituting (42) into (33), we obtain an explicit relation between $p_{s,out}$ and $p_{c,out}$ as

$$\frac{P_s\varepsilon_1 + P_d\varepsilon_2\gamma_s}{P_s\varepsilon_1}p_{s,out} + \frac{\gamma_s\varepsilon_2}{\gamma_1(\varepsilon_1+\varepsilon_2)}p_{c,out} = 1. \tag{43}$$

3) Achievable G-SDG: In this section, we first give an upper bound and a lower bound on the total outage probability of the MF scheme. Fortunately, both bounds lead to the same G-SDG, which is also the best diversity gain in theory.

Upper Bound and Lower Bound for Achievable p_t:

It is difficult to directly calculate the total outage probability due to the dependence between $p_{c,out}$ and $p_{s,out}$. Therefore, we analyze an upper bound and lower bound on the total outage probability, with the MF scheme. According to the definition, we can obtain an upper bound:

$$p_t = \Pr(E_A) + \Pr(E_B) + \Pr(E_C) \leq \Pr(E_A \cup E_C) + \Pr(E_B \cup E_C) \tag{44}$$

$$= p_{c,out} + p_{s,out} \leq 2\max\{p_{c,out}, p_{s,out}\}. \tag{45}$$

On the other hand, either secrecy outage or connection outage means the outage of the transmission. Therefore, we have a lower bound:

$$p_t \geq \max\{p_{c,out}, p_{s,out}\}. \tag{46}$$

We can see that the lower bound is one-half of the upper bound.

Achievable G-SDG:

With the generalized secure diversity gain defined in (24), the diversity gain is the same for both the upper bound and the lower bound on p_t since they only differ by a constant coefficient,

and it can be calculated as follows:

$$G\text{-}SDG(\rho) = \limsup_{SNR\to\infty} \frac{-\log(\max[p_{c,out}(SNR,\rho), p_{s,out}(SNR,\rho)])}{\log(SNR)} \tag{47}$$

$$= \limsup_{SNR\to\infty} \frac{-\max[\log p_{c,out}(SNR,\rho), \log p_{s,out}(SNR,\rho)]}{\log(SNR)} \tag{48}$$

$$= \limsup_{SNR\to\infty} \frac{\min[-\log((\frac{1}{\varepsilon_1}+\frac{1}{\varepsilon_2})\frac{\gamma_1}{SNR}), -\log(\frac{P_s\varepsilon_1}{P_s\varepsilon_1+P_d\varepsilon_2\gamma_s}(1-\frac{\gamma_s}{SNR\varepsilon_1}))]}{\log(SNR)} \tag{49}$$

$$= \min\left[1, \limsup_{SNR\to\infty} \frac{-\log(\frac{SNR\varepsilon_1}{SNR\varepsilon_1+SNR^{\rho}\varepsilon_2\gamma_s})}{\log(SNR)}\right] \tag{50}$$

$$= \begin{cases} 0 & \text{If } \rho \le 1 \\ \rho - 1 & \text{If } 1 < \rho \le 2 \\ 1 & \text{If } \rho > 2 \end{cases}. \tag{51}$$

By comparing the upper bound on G-SDG in (35) and the achievable G-SDG in (47), we have the following theorem.

Theorem 3: The modulo-and-forward scheme achieves the full generalized secrecy diversity gain for the untrusted relay channel.

D. Comparison with AF Scheme

This section compares the outage performance of the AF scheme with that of the MF scheme[7]. Since the secrecy outage probability is independent of the forwarding strategy at the relay, we need only to calculate the connection outage probability of the AF scheme, $p_{c,out}^{AF}$. From the received end-to-end SNR expression for the AF relaying, we can derive the connection outage probability as

$$p_{c,out}^{AF} = \Pr\left(\frac{P_s^2 g_1 g_2}{\sigma^2[P_s g_1 + (P_s+P_d)g_2 + \sigma^2]} < \gamma_o\right) \tag{52}$$

$$= 1 - e^{-\frac{\gamma_o\sigma^2}{P_s}\left(\frac{(P_s+P_d)}{P_s\varepsilon_1}+\frac{1}{\varepsilon_2}\right)} \frac{2\gamma_o\sigma^2}{P_s}\sqrt{\frac{1}{\varepsilon_1\varepsilon_2}\left(\frac{P_s+P_d}{P_s}+\frac{1}{\gamma_o}\right)} K_1\left(\frac{2\gamma_o\sigma^2}{P_s}\sqrt{\frac{1}{\varepsilon_1\varepsilon_2}\left(\frac{P_s+P_d}{P_s}+\frac{1}{\gamma_o}\right)}\right), \tag{53}$$

where the derivation from (52) to (53) is provided in Appendix II.

[7]The DF scheme is not compared since it cannot be adopted without CSIT.

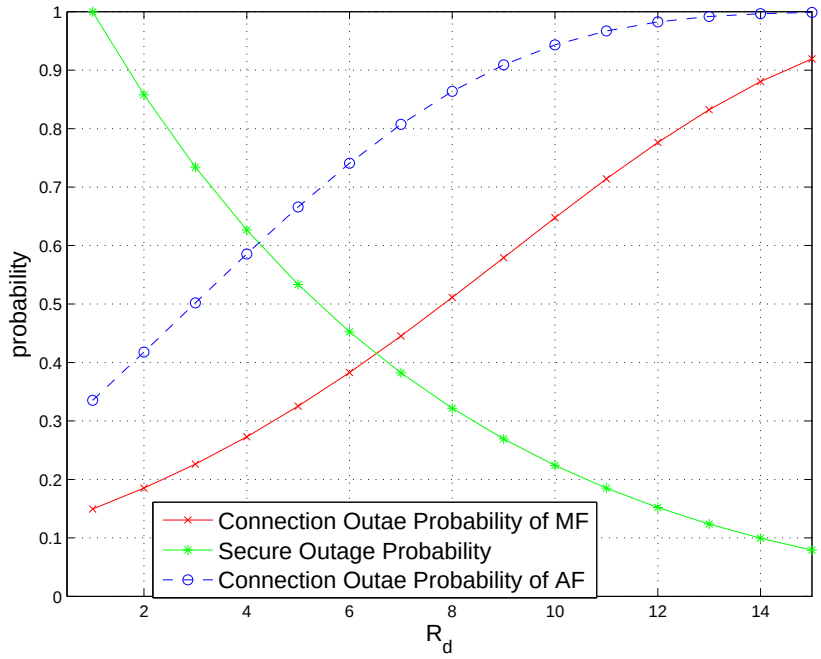

Fig. 5. Outage probabilities with MF and AF forwarding.

In Fig. 5, we plot the outage probability performance of the AF scheme and the MF scheme, where we set $P_s = P_d = 10$, $\varepsilon_1 = \varepsilon_2 = \sigma^2 = 1$, $R_s = 1/2$, and R_d varies from 1/2 to 15. We can see that there is a tradeoff between the connection outage and secrecy outage probabilities for both AF and MF schemes. However, the connection outage probability of the MF scheme is almost half that of the AF scheme with the same R_d, indicating that MF scheme is much more attractive for data transmission.

Secondly, we calculate the outage diversity gain of the AF scheme. When the SNR goes to infinity, $p_{c,out}^{AF}$ goes to zero only when $\rho \leq 2$. In this case, the asymptotic expression can be written as

$$p_{c,out}^{AF} \simeq \frac{\gamma_o \sigma^2}{P_s} \left(\frac{(P_s + P_d)}{P_s \varepsilon_1} + \frac{1}{\varepsilon_2} \right).$$

Similar to (47), we can calculate the outage diversity of the AF scheme as

$$DG_{af}(\rho) = -\limsup_{SNR\to\infty} \frac{-\log(\max[p_{c,out}^{AF}(SNR,\rho), p_{s,out}(SNR,\rho)])}{\log(SNR)} \tag{54}$$

$$= \min\Big[\limsup_{SNR\to\infty} \frac{-\log\left(\frac{\gamma_o}{SNR}\left(\frac{(SNR+SNR^{\rho})}{SNR\varepsilon_1}+\frac{1}{\varepsilon_2}\right)\right)}{\log SNR}, \limsup_{SNR\to\infty} \frac{-\log(\frac{SNR\varepsilon_1}{SNR\varepsilon_1+SNR^{\rho}\varepsilon_2\gamma_s})}{\log(SNR)}\Big] \tag{55}$$

$$= \begin{cases} 0 \quad \text{If } \rho \leq 1 \\ \rho - 1 \quad \text{If } 1 < \rho \leq 1.5 \\ 2-\rho \quad \text{If } 1.5 < \rho \leq 2 \\ 0 \quad \text{If } \rho \geq 2 \end{cases}. \tag{56}$$

Obviously, the maximum outage diversity of the AF scheme is $1/2$, which is only half of that of the MF scheme. Moreover, this diversity of $1/2$ is achieved only when $\rho = 3/2$, which requires very strict power control at the destination. These phenomena can be numerically observed in Fig. 6, where a comparison of generalized secure diversity gain between the the AF and the MF schemes is plotted.

VI. Conclusion

In this paper, we have considered the untrusted relay channel. Inspired by the MLAN channel, we have proposed a modulo operation before forwarding at the relay, at which a lattice encoded confidential message from the source and Gaussian distributed artificial noise from the destination are superimposed. As a result, the artificial noise only helps to protect the confidential message from eavesdropping at the untrusted relay, with almost no detrimental effect of wasted relay power. For the case with full CSIT, we have shown that the proposed MF scheme approaches the secrecy capacity within $1/2$ bit for any channel realization, hence achieving full generalized secure degrees of freedom. For the case without CIST, we have shown that the proposed MF scheme achieves the full generalized secure diversity gain of 1. On the other hand, the traditional AF scheme only achieves a G-SDG of $1/2$ at most.

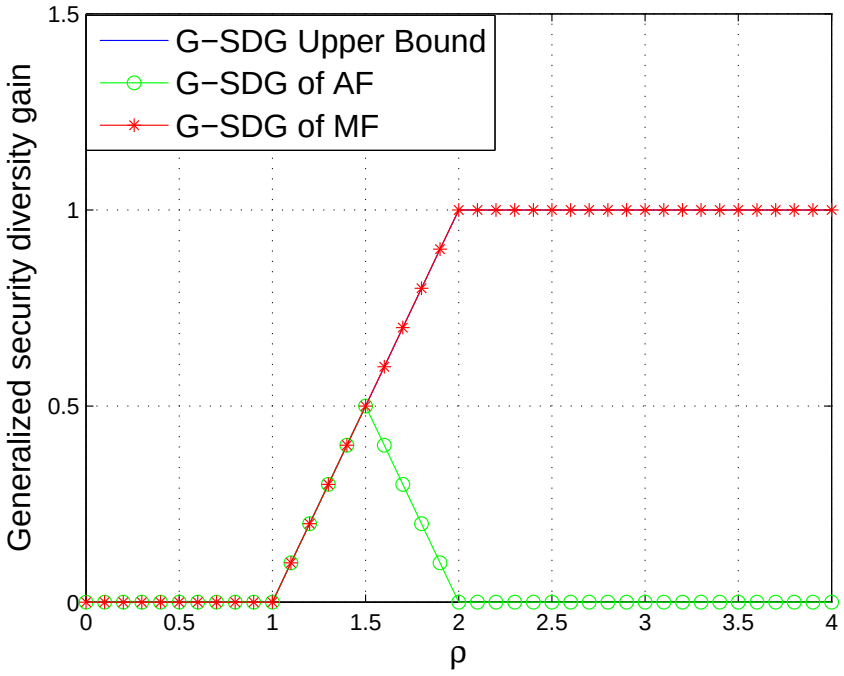

Fig. 6. Generalized secure diversity gain of AF and MF scheme versus ρ.

APPENDIX A
DERIVATION OF EQ. (41)

From (40), we can write the achievable connection outage probability as

$$p_{c,out} = \Pr\left[\frac{P_s}{\sigma^2}\frac{g_1 g_2}{g_1+g_2} < \gamma_1\right], \tag{A.1}$$

where $\gamma_1 = 2^{2R_d} - 1/2$ is the target SNR threshold. We can further write p_o as

$$\begin{aligned} p_{c,out} &= \Pr\left(g_1 g_2 < \frac{\gamma_1\sigma^2}{P_s}g_1 + \frac{\gamma_1\sigma^2}{P_s}g_2\right) \\ &= \Pr\left[g_1(g_2 - \frac{\gamma_1\sigma^2}{P_s}) < \frac{\gamma_1\sigma^2}{P_s}g_2\right]. \end{aligned} \tag{A.2}$$

Considering the two cases of $g_2 \le \frac{\gamma_1\sigma^2}{P_s}$ and $g_2 > \frac{\gamma_1\sigma^2}{P_s}$, we can rewrite $p_{c,out}$ as

$$p_{c,out} = \Pr\left(g_2 \le \frac{\gamma_1\sigma^2}{P_s}\right) + \Pr\left(g_2 > \frac{\gamma_1\sigma^2}{P_s}, g_1 < \frac{\frac{\gamma_1\sigma^2}{P_s}g_2}{g_2 - \frac{\gamma_1\sigma^2}{P_s}}\right). \tag{A.3}$$

Applying the probability density functions $f_{g_1}(x)=\frac{1}{\varepsilon_1}e^{-\frac{x}{\varepsilon_1}}$ and $f_{g_2}(x)=\frac{1}{\varepsilon_2}e^{-\frac{x}{\varepsilon_2}}$ in the above equation, we can obtain an analytical expression for the outage probability as

$$\begin{aligned} p_{c,out} &= \Pr\left(g_2 \le \frac{\gamma_1\sigma^2}{P_s}\right) + \int_0^{\frac{\frac{\gamma_1\sigma^2}{P_s}g_2}{g_2-\frac{\gamma_1\sigma^2}{P_s}}} f_{g_1}(g_1)\Pr\left(g_2 > \frac{\gamma_1\sigma^2}{P_s}\right)dg_1 \\ &= 1-\frac{1}{\varepsilon_2}\int_{g_2=\frac{\gamma_1\sigma^2}{P_s}} e^{-\left(\frac{1}{\varepsilon_2}+\frac{\gamma_1\sigma^2}{P_s\varepsilon_1(g_2-\frac{\gamma_1\sigma^2}{P_s})}\right)g_2}dg_2 \qquad \text{(A.4)} \\ &= 1-e^{-(\frac{1}{\varepsilon_1}+\frac{1}{\varepsilon_2})\frac{\gamma_1\sigma^2}{P_s}}\frac{2\gamma_1\sigma^2}{P_s\sqrt{\varepsilon_1\varepsilon_2}}K_1\Big(\frac{2\gamma_1\sigma^2}{P_s\sqrt{\varepsilon_1\varepsilon_2}}\Big). \qquad \text{(A.5)} \end{aligned}$$

Thus, we have (41).

APPENDIX B
DERIVATION OF EQ. (53)

From (52), we can write the connection outage probability of AF relaying as

$$\begin{aligned} p_{c,out}^{AF} &= \Pr\left(P_s^2 g_1 g_2 < P_s\sigma^2\gamma_o g_1 + (P_s+P_d)\sigma^2\gamma_o g_2 + \gamma_o\sigma^4\right) \qquad \text{(B.1)} \\ &= \Pr\left[(P_s^2 g_2 - P_s\sigma^2\gamma_o)g_1 < (P_s+P_d)\sigma^2\gamma_o g_2 + \gamma_o\sigma^4\right]. \qquad \text{(B.2)} \end{aligned}$$

Considering the two cases of $g_2 \le \frac{\gamma_o\sigma^2}{P_s}$ and $g_2 > \frac{\gamma_o\sigma^2}{P_s}$ separately, we can further write $p_{c,out}^{AF}$ as

$$\begin{aligned} p_{c,out}^{AF} &= \Pr(g_2 \le \frac{\gamma_o\sigma^2}{P_s}) + \Pr\left(g_2 > \frac{\gamma_o\sigma^2}{P_s}, g_1 < \frac{\gamma_o\sigma^2}{P_s}\cdot\frac{(P_s+P_d)g_2+\sigma^2}{P_s g_2-\gamma_o\sigma^2}\right) \qquad \text{(B.3)} \\ &= 1-\frac{1}{\varepsilon_2}\int_{\frac{\gamma_o\sigma^2}{P_s}}^{\infty} e^{-\frac{g_2}{\varepsilon_2}-\frac{\gamma_o\sigma^2}{P_s\varepsilon_1}\cdot\frac{(P_s+P_d)g_2+\sigma^2}{P_s g_2-\gamma_o\sigma^2}}dg_2. \qquad \text{(B.4)} \end{aligned}$$

Using the variable substitution of $x = g_2 - \frac{\gamma_o\sigma^2}{P_s}$, we can obtain a closed-form expression for the connection outage probability for the AF relaying as

$$p_{c,out}^{AF} = 1-e^{-\frac{\gamma_o\sigma^2}{P_s}\left(\frac{(P_s+P_d)}{P_s\varepsilon_1}+\frac{1}{\varepsilon_2}\right)}\frac{2\gamma_o\sigma^2}{P_s}\sqrt{\frac{1}{\varepsilon_1\varepsilon_2}\Big(\frac{P_s+P_d}{P_s}+\frac{1}{\gamma_o}\Big)}K_1\left(\frac{2\gamma_o\sigma^2}{P_s}\sqrt{\frac{1}{\varepsilon_1\varepsilon_2}\Big(\frac{P_s+P_d}{P_s}+\frac{1}{\gamma_o}\Big)}\right). \qquad \text{(B.5)}$$

In this way, the proof of (53) has been completed.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1948.

[2] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[3] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[4] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Sep. 2005, pp. 2152–2155.

[5] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Sep. 2008.

[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 356–360.

[7] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[8] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[9] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 532–540, Sep. 2011.

[10] L.-C. Choo, C. Ling, and K.-K. Wong, "Achievable rates for lattice coding over the Gaussian wiretap channel," in *Proc. IEEE Int. Conf. Communications*, Jun. 2011, pp. 1–5.

[11] X. He and A. Yener, "Providing secrecy with lattice codes," in *Proc. 46th Annual Allerton Conf. Communication, Control and Computing*, Sep. 2008, pp. 1199–1206.

[12] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[13] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Commun. Letter*, vol. 14, no. 8, pp. 752–754, Aug. 2010.

[14] S. Zhang, S. Liew, and P. Lam, "Physical layer network coding," in *Proc. ACM Mobicom 2006, LA*, Sep. 2006.

[15] K. Lu, S. Fu, Y. Qian, and T. Zhang, "On the security performance of physical-layer network coding," in *Proc. IEEE Int. Conf. Communications*, Jun. 2009, pp. 1–5.

[16] A. Mukherjee and A. Swindlehurst, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *Proc. IEEE Workshop on Signal Processing Advances in Wireless Communications*, Jun. 2010, pp. 1–5.

[17] J. Huang, A. Mukherjee, and A. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

[18] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE Global Conf. Communications*, Nov. 2008, pp. 1–5.

[19] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[20] X. He and A. Yener, "End-to-end secure multi-hop communication with untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 1–11, Jan. 2013.

[21] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[22] C. Jeong, I.-M. Kim, and D. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward mimo untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[23] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+\mathrm{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.

[24] A. Ozgur and S. Diggavi, "Approximately achieving Gaussian relay network capacity with lattice-based QMF codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8275–8294, Dec. 2013.

[25] S. Jafar and S. Vishwanath, "Generalized degrees of freedom of the symmetric Gaussian K user interference channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3297–3303, Jul. 2010.

[26] L. Sun, T. Zhang, Y. Li, and N. H, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[27] J. Vicario, A. Bel, J. Lopez-Salcedo, and G. Seco, "Opportunistic relay selection with outdated CSI: outage probability and diversity analysis," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 2872–2876, Jun. 2009.

[28] C. Lo, S. Vishwanath, and R. Heath, "Relay subset selection in wireless networks using partial decode-and-forward transmission," *IEEE Trans. Veh. Technol.*, vol. 58, no. 2, pp. 692–704, Feb. 2009.